# PATENT ABSTRACTS OF JAPAN

(11)Publication number : **06-069882**

(43)Date of publication of application : **11.03.1994**

(51)Int.Cl. **H04B 7/26**

**H04L 9/06**

**H04L 9/14**

(21)Application number : **04-220386**

(22)Date of filing : **19.08.1992**

(71)Applicant : **NIPPON TELEGR & TELEPH CORP <NTT>**

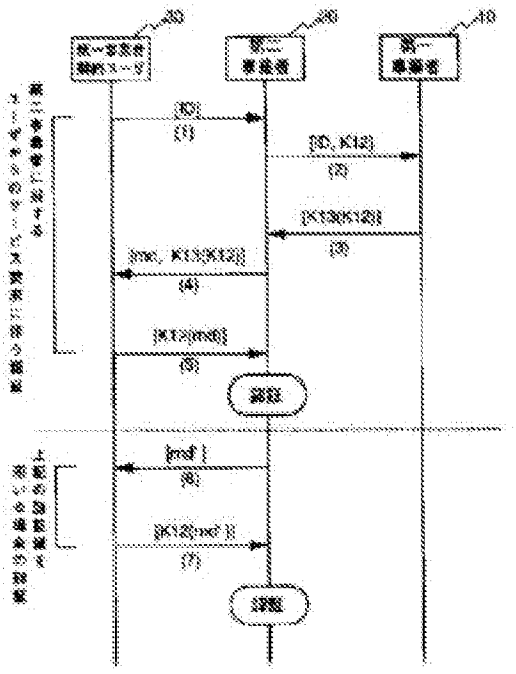
(72)Inventor : **SUZUKI SHIGEFUSA**
**NOHARA TATSUO**

(54) **CERTIFYING METHOD FOR MOBILE COMMUNICATION SYSTEM**

(57)Abstract:

PURPOSE: To secure the privacy of a certification key shared with a mobile subscriber by performing certification corresponding to a signal receiving and ciphering a temporary certification key from a second mobile communication network in the case of subscriber certification for roaming.

CONSTITUTION: When a mobile subscriber 30 moves from a first mobile communication network to a second mobile communication network 20, an identification number ID is transmitted for getting subscriber certification. The second network sends this ID and a set certification key K12 to the first network 10, and the first network returns a certification key K13 ciphered by the K12 to the second network in place of directly sending the certification key K12 shared with the subscriber 30. The second network 20 stores the K13, sends a random value to the subscriber 30, collates the random number value provided by restoring a certification response signal ciphered by the K13 by using the K12 and certifies the identity of the subscriber by the coincidence. Thus, since the certification key K13 is used only for ciphering, the privacy can be secured.



(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平6－69882

(43)公開日　平成6年(1994)3月11日

| (51)Int.Cl.[5] | | 識別記号 | 庁内整理番号 | ＦＩ | 技術表示箇所 |
|---|---|---|---|---|---|
| Ｈ０４Ｂ | 7/26 | １０９　Ｓ | 7304－5K | | |
| | | Ａ | 7304－5K | | |
| Ｈ０４Ｌ | 9/06 | | | | |
| | 9/14 | | | | |
| | | | 7117－5K | Ｈ０４Ｌ　9/ 02 | Ｚ |

審査請求　未請求　請求項の数2(全 10 頁)

(21)出願番号　特願平4－220386

(22)出願日　平成4年(1992)8月19日

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区内幸町一丁目1番6号

(72)発明者　鈴木　茂房
東京都千代田区内幸町1丁目1番6号　日本電信電話株式会社内

(72)発明者　野原　龍男
東京都千代田区内幸町1丁目1番6号　日本電信電話株式会社内

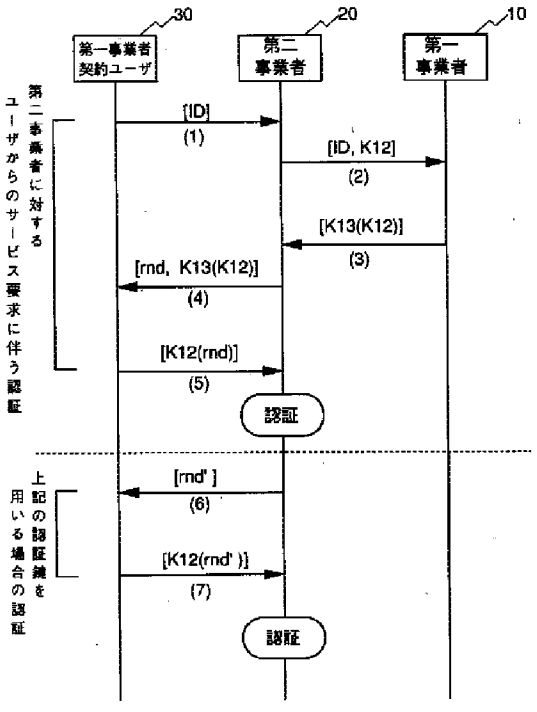
(74)代理人　弁理士　澤井　敬史

(54)【発明の名称】　移動通信方式における認証方法

(57)【要約】

【目的】　異なる事業者がサービスする移動通信網に移行した時にもサービスが受けられる、いわゆるローミングを行う際の加入者認証において、契約事業者との間で共有する移動加入者の認証鍵を移行先の事業者に漏らさないようにする。

【構成】　移動加入者が、第一の事業者がサービスする第一の移動通信網で通信中に、他事業者がサービスする第二の移動通信網に移行して通信を続行する際、この第二の網で加入者認証を受けるために移動機識別番号を送信した時、第二の網はこの識別番号及び認証鍵を第一の網に送り、第一の網は第二の網に移動加入者と共有する認証鍵を直接送る代わりにこの受信した認証鍵で暗号化した信号を返送し、第二の網はこれを用いて認証を行うことにより、第一の事業者と移動加入者間で共有する認証鍵が第二の網に漏れることが防止できる。



【特許請求の範囲】
【請求項１】　移動局が正規の移動加入者であることを認証により確認した後にこの移動加入者と通信を開始する第一の移動通信網と、この移動通信網と通信回線で接続される第二の移動通信網とを含み、前記移動局と前記第一の移動通信網は前記移動局を認証するための第一の認証鍵を共有し、かつ前記移動局が前記第二の移動通信網とも接続資格を有する場合に前記第二の移動通信網が前記移動局の認証を行うための方法であって、
前記移動局は前記第二の移動通信網に対してこの移動局の移動局識別番号を送信し、これを受けた前記第二の移動通信網はこの受信した移動局識別番号と第二の認証鍵を前記第一の移動通信網に送信するとともに前記第二の認証鍵を前記第一の認証鍵で暗号化した信号である認証信号を前記第一の移動通信網から受信したらこの認証信号と乱数値とを前記移動局に送信し、これを受けた前記移動局は予め具備している前記第一の認証鍵を用いて前記認証信号を復号して前記第二の認証鍵を復元した上でこの第二の認証鍵で前記乱数値を暗号化した信号である認証応答信号を前記第二の移動通信網に送信し、前記第二の移動通信網はこの認証応答信号により前記移動局の認証を行うことを特徴とする移動通信方式における認証方法。
【請求項２】　移動局が正規の移動加入者であることを認証により確認した後にこの移動加入者と通信を開始する第一の移動通信網と、この第一の移動通信網と通信回線で接続される第二の移動通信網とを含み、前記移動局と前記第一の移動通信網は前記移動局を認証するための第一の認証鍵を共有し、かつ前記移動局が前記第二の移動通信網とも接続資格を有する場合に前記第二の移動通信網が前記移動局の認証を行うための方法であって、
前記移動局は前記第二の移動通信網に対してこの移動局の移動局識別番号を送信し、これを受けた前記第二の移動通信網はこの受信した移動局識別番号と第二の認証鍵を第三の認証鍵で暗号化した鍵信号を前記第一の移動通信網に送信するとともに前記鍵信号を前記第一の認証鍵で暗号化した信号である認証信号を前記第一の移動通信網から受信したらこの認証信号と乱数値と前記第三の認証鍵とを前記移動局に送信し、これを受けた移動局は予め具備している前記第一の認証鍵と受信した前記第三の認証鍵とを用いて前記認証信号を復号して前記第二の認証鍵を復元した上でこの第二の認証鍵で前記乱数値を暗号化した信号である認証応答信号を前記第二の移動通信網に送信し、前記第二の移動通信網はこの認証応答信号により前記移動局の認証を行うことを特徴とする移動通信方式における認証方法。
【発明の詳細な説明】
【０００１】
【産業上の利用分野】本発明は異なる通信事業者がそれぞれ独自の移動通信網を構築して移動通信サービスを提供している場合に、特定の移動加入者がそれらの複数の通信事業者のサービスを受ける（いわゆるローミング）ための加入者認証方法に関する。
【０００２】
【従来の技術】図２に従来の技術及び本発明の前提となる移動通信システムの構成図を示す。１０は移動通信サービスを提供する第一の事業者が構築した第一の移動通信網、１１はこの第一の移動通信網に含まれる基地局又は交換局、１２は第一の移動通信網のサービスエリア、２０は移動通信サービスを提供する第二の事業者が構築した第二の移動通信網、２１はこの第二の移動通信網に含まれる基地局又は交換局、２２は第二の移動通信網のサービスエリア、３０は本来第一の事業者の加入者であって第二の事業者のローミングサービスも受けられるように契約してある移動加入者、４０は第一の移動通信網と第二の移動通信網を接続する通信回線である。各移動通信網は自分のサービスエリアであることを示す報知情報を常時送信している。従って、移動加入者３０はその報知情報を受信することによって、どこの移動通信網のエリアにいるのかがわかる。もちろん第一の移動通信網から第二の移動通信網に移行することもわかる。
【０００３】現在、実用化されている移動通信サービスでは異なる事業者間のローミングサービスは行われていないから、これに関する従来技術はない。そこで従来の自動車電話方式における加入者認証技術を上記の網移行時における認証に単純に適用した場合の手順を従来技術として図３に示す。ここで３０は第一事業者に加入契約しておりかつ第二事業者からローミングサービスを受けられる移動加入者であり、１０と２０は第２図の場合と同一である。
【０００４】移動加入者（以下、単に加入者と称する）３０はゾーン移行を検出すると自分の移動機識別番号〔ＩＤ〕を移行先の第二の移動通信網（以下、単に第二の網という）に向けて送信する（工程１）。この〔ＩＤ〕は加入者３０と第一の事業者との間で決めたこの加入者を識別するための番号である。これを受信した第二の網は、この移動加入者がローミングサービス可能な加入者か否かを確認し、可能な場合に第一の移動通信網（以下、単に第一の網という）にこの〔ＩＤ〕を通信回線４０を用いて送信する（工程２）。これを受けた第一の網は加入者３０との間で共有している認証鍵〔Ｋ１３〕を第二の網に送信する（工程３）。第二の網はこの〔Ｋ１３〕を記憶するとともに認証用に乱数値を発生させ、その乱数値を加入者３０に送信する（工程４）。これを受けた加入者３０はこの乱数値を認証鍵〔Ｋ１３〕で暗号化し、その暗号化した信号である認証応答信号を第二の網に送信する（工程５）。第二の網はこの認証応答信号を受信したら、工程３の後に記憶しておいた認証鍵〔Ｋ１３〕を用いて復号し、復号した乱数値と工程４で加入者３０に送った乱数値とを照合して一致したら、

加入者３０が正規の加入者であると認証できたことになる。これにより第二の網は〔ＩＤ〕と〔Ｋ１３〕との関係を記憶しておけば、呼接続のたびに必要な認証を行うことができる。この認証は、上記の工程４と工程５の手順により実行できる。

【０００５】

【発明が解決しようとする課題】上記従来の技術では、加入者と第一の移動通信網で共有している認証鍵を、全く別の業者が運営する第二の移動通信網に通知する必要があるから、認証鍵の守秘性の点で問題があった。本発明は、認証鍵の守秘性を確保したままローミングサービスにおける加入者認証を行う新たな認証方法を提供することを目的とする。

【０００６】

【課題を解決するための手段】本発明の認証方法は、第二の移動通信網がこの認証のための仮の認証鍵を第一の移動通信網に送り、第一の移動通信網はこの仮の認証鍵を移動加入者との間で共有する認証鍵で暗号化し、その暗号化信号を用いて移動加入者の認証を行う点を特徴とする。

【０００７】

【作用】本発明では、第一の移動通信網は移動加入者との間で共有する認証鍵を第二の移動通信網に直接通知するのではなく、第二の移動通信網から受信した仮の認証鍵を暗号化した信号を通知すればよいから、移動加入者との間で共有する認証鍵の守秘性を確保することができる。

【０００８】

【実施例】図１は本発明における認証方法の第一の例である。記載方法は図３の場合と同一である。移動加入者（以下、単に加入者という）３０が第一の移動通信網（以下、第一の網という）から第二の移動通信網（以下、第二の網という）に移行したことを検出して、自分の識別番号〔ＩＤ〕を第二の網に送信するまで（工程１）は従来と同一である。移行の検出も各網が報知している情報に基づいて実行できることも従来どおりである。本発明で対象とする移動通信網として、無線回線制御を行う基地局と加入者のデータを保持する記憶装置が必要である。

【０００９】加入者３０から〔ＩＤ〕を受信した第二の網はこの〔ＩＤ〕と第二の網と加入者３０との間で共有する認証鍵〔Ｋ１２〕を設定して第一の網に送信する（工程２）。従来は〔ＩＤ〕だけを送信していたのに対して認証鍵〔Ｋ１２〕も送信する点が従来と異なる。第一の網はこれを受けると、認証鍵〔Ｋ１２〕を加入者３０と共有する認証鍵〔Ｋ１３〕で暗号化し、その暗号化した信号である認証信号を第二の網に返送する（工程３）。これを受けた第二の網は、乱数値を発生させ、その乱数値と上記の認証信号を加入者３０に送信する（工程４）。これを受けた加入者３０は認証鍵〔Ｋ１３〕を用いて暗号化信号を復号して認証鍵〔Ｋ１２〕を復元し、それを用いて受信した乱数値を暗号化して認証応答信号を生成し、その認証応答信号を第二の網に返送する（工程５）。第二の網はこの認証応答信号を認証鍵〔Ｋ１２〕を用いて復号して乱数値を復元し、それと工程４で送信した乱数値とを比較照合し、一致したら加入者３０を正規の加入者として認証する。もしくは、第二の網は工程４で送信した乱数値を認証鍵〔Ｋ１２〕を用いて暗号化し、この値と認証応答信号とを比較照合し、一致したら加入者３０を正規の加入者として認証する。この認証が完了したら、第二の網はこの加入者の識別番号〔ＩＤ〕と認証鍵〔Ｋ１２〕との関係を記憶しておくことにより、工程６と工程７に示すように以降の加入者３０との呼接続の際に認証を行うことができる。

【００１０】この例によれば、認証鍵〔Ｋ１２〕は公開されるが、認証鍵〔Ｋ１３〕は認証鍵〔Ｋ１２〕を暗号化するために用いられているだけであるから、〔Ｋ１３〕の秘匿性を確保することができる。〔Ｋ１２〕は第二の網が加入者３０との間で仮に設ければよい鍵であるから公開してもそれほど問題ない。加入者３０は第二の網の正規の加入者ではなく、あくまでローミング用の加入者であるから、鍵〔Ｋ１２〕の守秘の要求は大きくないからである。（加入者３０が第二の網の正規の加入者であれば、本発明を用いなくても従来の方法により認証できる。）　もし、〔Ｋ１２〕を秘匿したい場合には後述の第二の実施例によればよい。

【００１１】図４は上記の例の場合の移動加入者３０の制御手順である。工程Ｓ１はサービスゾーンを移行した時に報知情報を受信して移行先のサービス事業者を判定する部分である。加入者３０は在圏している事業者名を記憶しているから、移行先の事業者名と記憶中のそれとを比較することにより事業者判定が可能である。これが一致していれば、移行しても事業者が変わらない場合だから、後述の工程Ｓ５に移ればよい。不一致なら工程Ｓ２に移るが、この場合は異なる事業者のゾーンに移行した場合だから、移行先のゾーンが第一の事業者がどうかを調べる。第一の事業者であれば他の事業者のゾーンから戻った場合であり、工程Ｓ１３で認証鍵をＫ１３に設定して工程Ｓ５に移る。第一の事業者でなければ、本発明第一の例の場合と同一となり、工程Ｓ４で暗号解読鍵をＫ１３に設定する。これは図１に示す制御手順の中の工程４で、第２の網から送信される暗号化信号を復号するためである。この後に工程Ｓ５に移る。これは網へのサービス要求の部分であり、図１では工程１に相当する。ここでは加入者３０は第一の事業者との間で取り交わした識別番号〔ＩＤ〕を送信する。その後、図１を見ればわかるように第一の網と第２の網との間で所要の信号の授受を行った後、図１の工程４で記載のように網から乱数値と暗号化した信号からなる認証要求信号が送られるから、これを受信する工程になる。これがＳ６であ

る。例えば認証種別１＝乱数なし、認証種別２＝乱数有りのように種別分けされた情報があり、これにより区別する方法も考えられるから、この認証要求信号から、いかなる認証方式を行うのかを検出するのが工程Ｓ７である。つまり図１と図３の工程４を比較すればわかるように、加入者３０が異なる事業者のゾーンに移った場合は乱数値以外に暗号化した信号が送られるが（図１の工程４を参照）、同一事業者のゾーンの場合には乱数値だけが送られる（図３の工程４を参照）から、この内容を見れば異なる事業者のゾーンに移行したかどうかがわかるからである。乱数値以外の情報が含まれている場合には異なる事業者のゾーンに移行した場合だから、工程Ｓ８でその暗号化信号を復号して〔Ｋ１２〕を復元し、それを認証鍵にする。そうでない場合には認証鍵はそのままにする。その後工程Ｓ９で、認証鍵を用いて網へ認証応答を行う。もし異なる事業者へ移行した場合には新たな認証鍵〔Ｋ１２〕を用いて認証応答することになる。これが図１の工程５に相当する。

【００１２】図５は第二の例であり、上記の仮の鍵〔Ｋ１２〕も秘匿したい場合の認証手順である。ここでは第二の網は仮の鍵〔Ｋｔ〕を用い、工程２～工程４までのについて第一の例での鍵〔Ｋ１２〕の代わりに、この鍵を〔Ｋｔ〕で暗号化した信号〔Ｋｔ（Ｋ１２）〕を用いたことを特徴とする。その他の工程は第一の例と同一である。

【００１３】この例によれば、特に工程２において鍵〔Ｋ１２〕を送受信するのではなくて、これを鍵〔Ｋｔ〕で暗号化した信号を送受信するので、鍵〔Ｋ１３〕だけでなく〔Ｋ１２〕も秘匿できる。図６は本発明第１の実施例の具体的な適用例として、位置登録時に認証を行う場合を示す。ゾーン移行した時には移動加入者３０は位置登録を行うから、その時に本発明の認証動作を行う。なお、これまでの既述では第一事業者等は第一の移動通信網等として説明していたが、ここでは第一事業者等として説明する。どちらでも本発明の要旨を変えることはないからである。

【００１４】まず移動加入者３０は移行先の移動通信網である第二事業者に対して位置登録要求信号を送信する（工程１）。当然この信号には移動加入者３０の識別番号〔ＩＤ〕を含む。この信号を受信した第二事業者２０はこの移動加入者用の認証鍵〔Ｋ１２〕を発生し、〔ＩＤ〕とともに通信回線を経由して第一事業者１０に送信する（工程２）。第一事業者１０は〔ＩＤ〕を検出して、加入者３０が自分の契約ユーザであることを確認したら、認証鍵〔Ｋ１２〕を移動加入者との間で共有する認証鍵〔Ｋ１３〕で暗号化した認証信号〔Ｋ１３（Ｋ１２）〕を第二事業者に送信する（工程３）。これを受けた第二事業者２０は認証用の乱数値を発生させ、それと認証信号をセットにして加入者３０に送信する（工程４）。移動加入者３０はこれを受けて、認証信号を認証鍵〔Ｋ１３〕で復号して鍵〔Ｋ１２〕を復元・記憶したうえで、この鍵〔Ｋ１２〕で第二事業者から受信した乱数値を暗号化した認証応答信号〔Ｋ１２（ｒｎｄ）〕を第二事業者に送信する（工程５）。第二事業者２０はこの認証応答信号を鍵〔Ｋ１２〕で復号して得た乱数値を、工程４で送信した乱数値と比較照合し、一致すればこの移動加入者３０がローミングサービス可能な加入者であると判断して、この加入者の〔ＩＤ〕と鍵〔Ｋ１２〕を記憶するとともに呼接続処理を可能とする。

【００１５】工程６～工程９は移動加入者３０から発呼要求があった場合の呼接続手順である。先ず加入者３０は発呼信号を第二事業者に送信する（工程６）。第二事業者はこれを受けて受付信号を加入者に返送する（工程７）とともに乱数値〔ｒｎｄ〕を含む認証要求信号を送信する（工程８）。加入者３０は記憶済の鍵〔Ｋ１２〕を用いたこの乱数値を暗号化し、それを認証応答信号として返送する（工程９）。第二事業者はここで認証を行い、完了したら回線接続処理に移る。この処理は従来の処理と同様であって、本発明の特徴ではないから省略する。

【００１６】本発明は、第一の網と第二の網を接続する通信回線を持たない場合でも、事前に、第二の網が第一の網から第一の網に属するすべての〔ＩＤ〕をオフラインで取得し、これを元に、第二の網が第一の網に、全ての〔ＩＤ〕とその〔ＩＤ〕を持つ加入者に対する一時的な認証鍵〔Ｋ１２〕をオフラインで通知し、さらにこれを元に、第一の網が第二の網に、その〔ＩＤ〕を持つ加入者の認証鍵〔Ｋ１３〕によって暗号化された〔Ｋ１３（Ｋ１２）〕をオフラインで通知することによっても達成される。ここで、オフラインとは、例えば郵便などが考えられる。

【００１７】

【発明の効果】本発明によれば、ローミング先の事業者が移動加入者を認証する際、第一事業者と加入者で共有する認証鍵〔Ｋ１３〕を直接に用いないで、第二事業者と加入者間で共有する鍵〔Ｋ１２〕を〔Ｋ１３〕で暗号化した信号を用いるようにしたから、鍵〔Ｋ１３〕を秘匿できる。さらに、鍵〔Ｋ１２〕さえも秘匿することも可能である。

【図面の簡単な説明】

【図１】本発明の第一の実施例を説明する図である。

【図２】本発明と従来の認証方法の双方の前提となるシステム構成図である。

【図３】従来の認証手順を示す図である。

【図４】本発明の第一の実施例で動作する移動局の動作手順を示す図である。

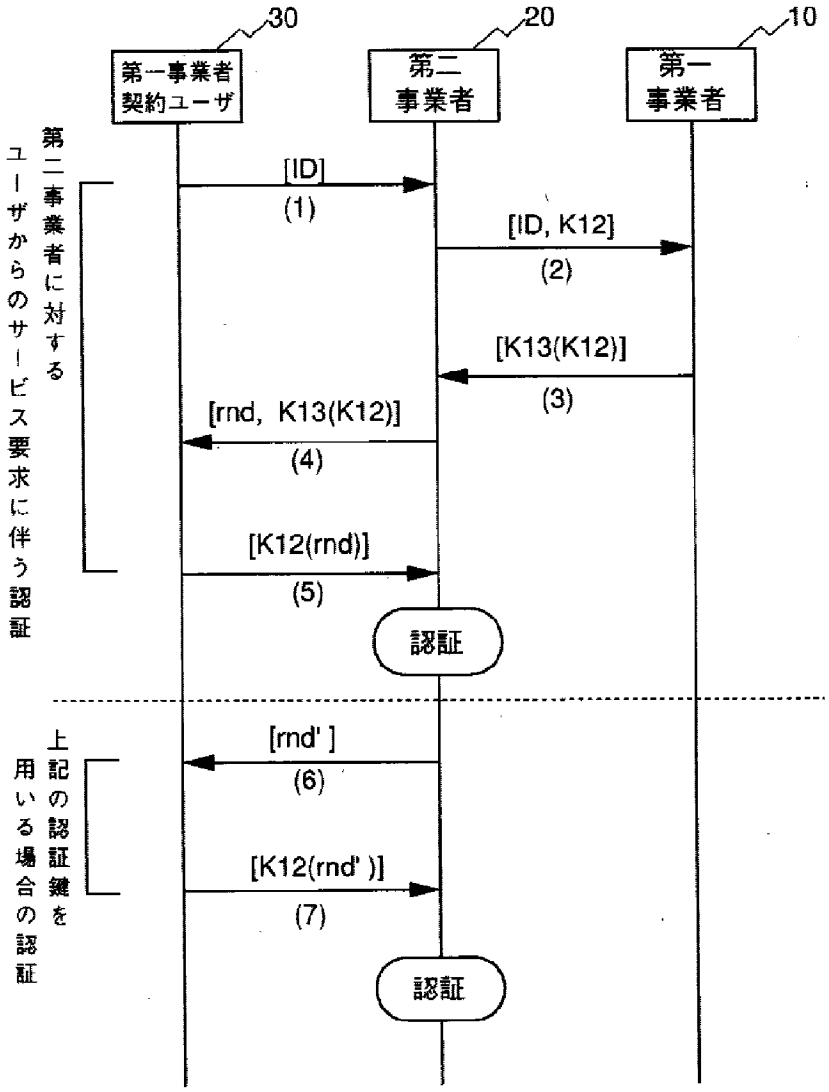
【図５】本発明の第二の実施例を示す図である。

【図６】位置登録の際に本発明の第一の実施例を実行する場合の制御手順である。

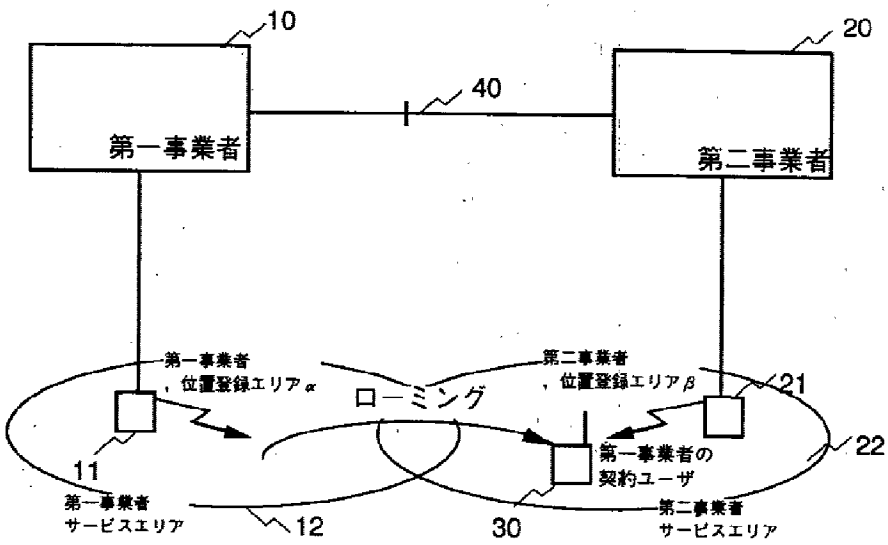
【符号の説明】

１０　　第一事業者　　３０　　移動加入者
２０　　第二事業者

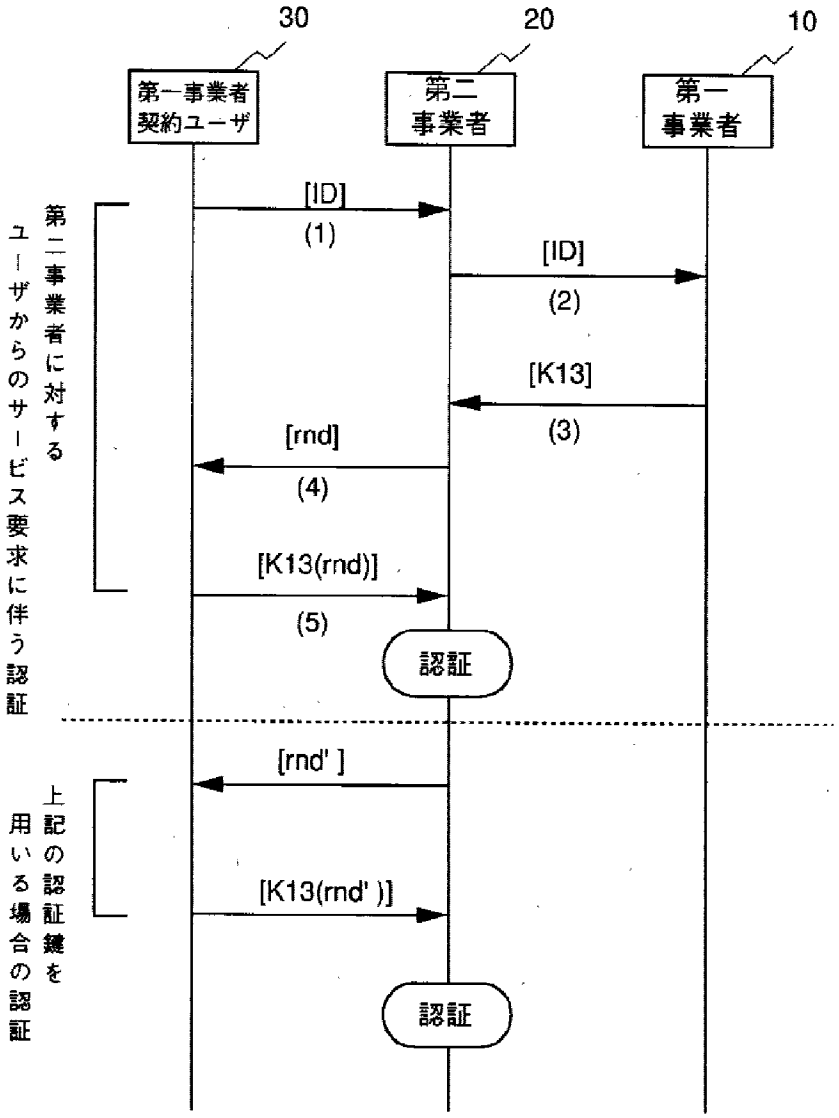
【図１】



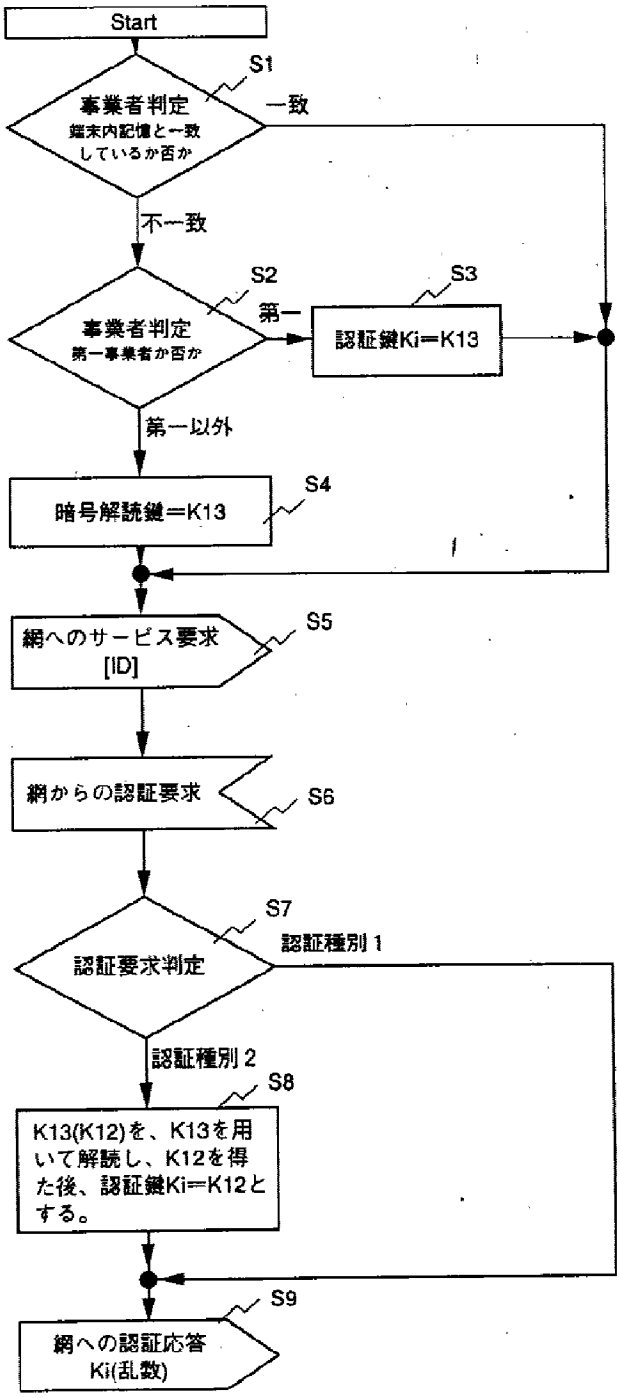
【図２】


10
20
40
第一事業者
第二事業者
第一事業者
，位置登録エリアα
ローミング
第二事業者
，位置登録エリアβ
21
22
11
第一事業者の
契約ユーザ
第一事業者
サービスエリア
12
30
第二事業者
サービスエリア

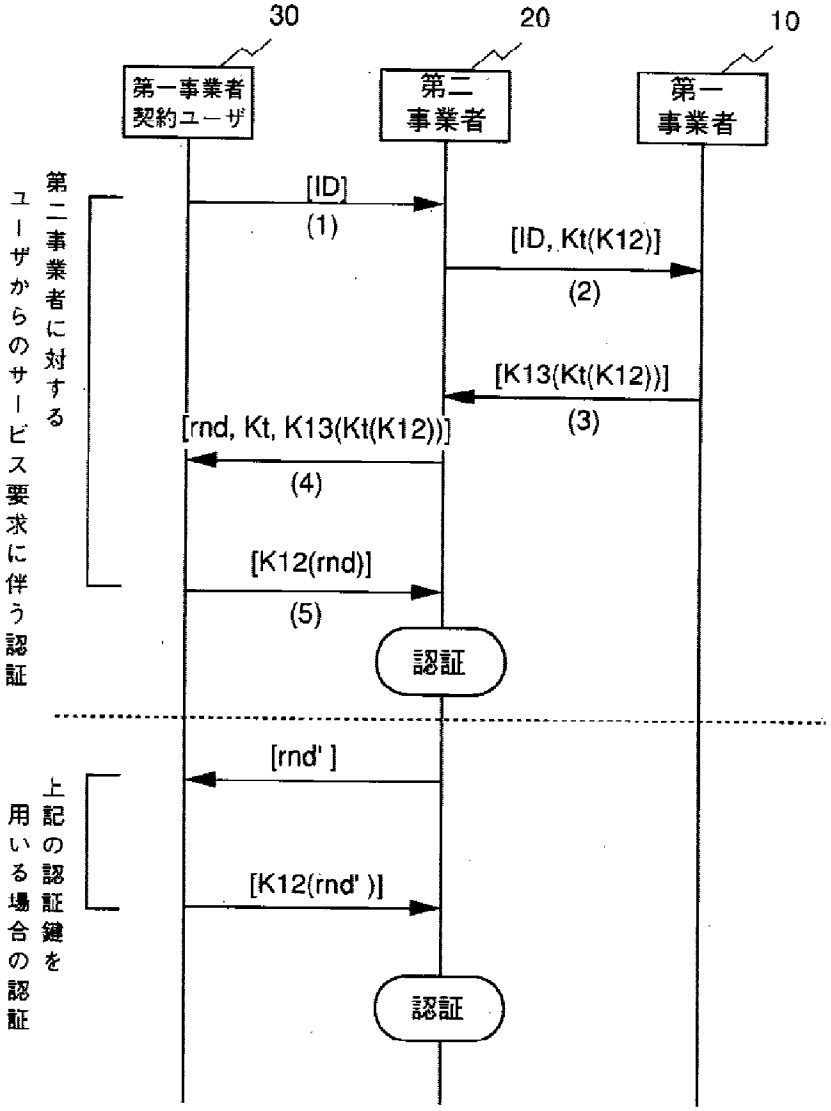
【図3】


30
20
10
第一事業者
契約ユーザ
第二
事業者
第一
事業者
[ID]
(1)
[ID]
(2)
[K13]
(3)
[rnd]
(4)
[K13(rnd)]
(5)
認証
[rnd' ]
[K13(rnd' )]
認証
第二事業者に対するユーザからのサービス要求に伴う認証
上記の認証鍵を用いる場合の認証

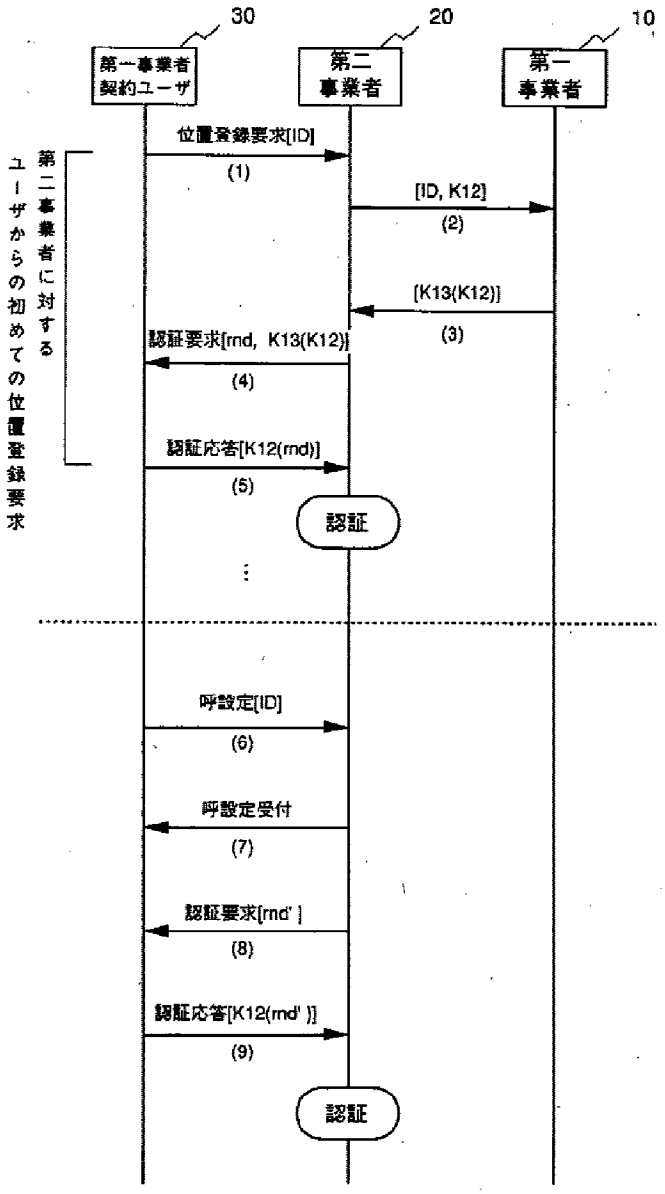
【図4】


Start
S1
事業者判定
端末内記憶と一致
しているか否か
一致
不一致
S2
事業者判定
第一事業者か否か
第一
S3
認証鍵Ki=K13
第一以外
暗号解読鍵=K13
S4
網へのサービス要求
[ID]
S5
網からの認証要求
S6
S7
認証要求判定
認証種別1
認証種別2
S8
K13(K12)を、K13を用
いて解読し、K12を得
た後、認証鍵Ki=K12と
する。
S9
網への認証応答
Ki(乱数)

【図５】


30
20
10
第一事業者
契約ユーザ
第二
事業者
第一
事業者
第二事業者に対する
ユーザからのサービス要求に伴う認証
[ID]
(1)
[ID, Kt(K12)]
(2)
[K13(Kt(K12))]
(3)
[rnd, Kt, K13(Kt(K12))]
(4)
[K12(rnd)]
(5)
認証
[rnd' ]
上記の認証鍵を
用いる場合の認証
[K12(rnd' )]
認証

【図６】


30
20
10
第一事業者
契約ユーザ
第二
事業者
第一
事業者
位置登録要求[ID]
(1)
[ID, K12]
(2)
[K13(K12)]
(3)
認証要求[rnd, K13(K12)]
(4)
認証応答[K12(rnd)]
(5)
第二事業者に対するユーザからの初めての位置登録要求
認証
呼設定[ID]
(6)
呼設定受付
(7)
認証要求[rnd']
(8)
認証応答[K12(rnd')]
(9)
認証